



# ENTERPRISE DATA DISCOVERY SERVICES BRIEF

*Find Sensitive Data. Reduce Unnecessary Risk.*

---

SPECIALIZED **S|3** SECURITY SERVICES

# HIDDEN DATA CREATES HIDDEN RISK

***Sensitive information rarely stays in one place.***

It gets downloaded for a project, copied into shared folders, stored in email, migrated to the cloud, retained in legacy systems, or left behind long after its original purpose has passed.

Over time, organizations can lose visibility into where sensitive information resides and whether it is being stored appropriately.

***That uncertainty creates risk.***

S3 Security's Enterprise Data Discovery service helps organizations identify sensitive, regulated, confidential, and proprietary information across supported on-premises and cloud environments. Our team works with you to determine what data matters, where to look for it, and performs discovery across your environment.

***But discovery is only the beginning of our service.***

S3 Security engineers review scan results to reduce false positives, work with your team to evaluate remaining findings, and help determine appropriate next steps. Where supported, we can also perform approved remediation and provide final reporting documenting what was identified, addressed, and remains outstanding.

Enterprise Data Discovery assessments gives your organization greater visibility into what sensitive information you have, where it resides, and whether it is encrypted, where it should be, helping you make better decisions about protection, retention, remediation, and risk.



***Visibility leads to better decisions about protection, remediation, and risk.***

# DISCOVER THE DATA THAT MATTERS

Every organization has different information to protect. S3 Security tailors each engagement around your business priorities, regulatory requirements, and risk profile to focus the search on the data that matters most.

## ***Search Based on Your Business and Risk***

We work with your team to define the data types and search criteria that matter to your business, regulatory requirements, and risk profile.

Discovery can be configured to identify common forms of sensitive and regulated information, including:

- **Personally Identifiable Information (PII)**
- **Protected Health Information (PHI)**
- **Payment Card Data**
- **Financial & Banking Information**
- **Government & Personal Identifiers**
- **Confidential Business Information**
- **Proprietary Information & IP**
- **Other Client-Defined Data**

Search criteria can also be customized to identify information unique to your organization, extending discovery beyond standard regulatory data types.

## ***Search Across the Enterprise***

Sensitive data can exist well beyond the systems where it is expected to reside. Depending on scope and technical requirements, S3 Security can conduct discovery across supported environments such as:

- **Servers & Workstations**
- **Databases**
- **Network & File Storage**
- **Email**
- **Microsoft 365 & Collaboration Platforms**
- **Cloud Storage & Environments**
- **Shared Repositories**
- **Other Supported Data Sources**

This breadth can help uncover forgotten, duplicated, misplaced, or otherwise unexpected stores of sensitive information.

***Discover your sensitive data wherever it resides.***

# OUR MANAGED DISCOVERY PROCESS

## *From Scoping Through Final Reporting*

S3 Security manages the discovery process from initial planning through analysis, remediation, and final reporting, working closely with your team at each stage.

1

### Scope the Discovery

We work with your team to define the sensitive, regulated, confidential, or proprietary information to search for and the systems, locations, repositories, and supported cloud environments to include.

2

### Prepare the Environment

S3 Security works with your team to establish the accounts, permissions, connectivity, and scanning infrastructure required. Depending on the environment, this may include installing scanning agents and coordinating scanning windows to minimize disruption.

3

### Conduct Discovery

S3 Security conducts discovery across the agreed-upon targets and consolidates results for analysis.

4

### Review and Validate

Our engineers review findings and eliminate as many false positives as possible before presenting results to your team. Together, we evaluate what is confirmed, what can be ruled out, and what may require further investigation.

5

### Remediate and Report

S3 Security discusses appropriate remediation options based on confirmed findings and the environment. Where supported, remediation is performed only with client authorization, followed by final reporting of what was identified, what was remediated, and what remains outstanding.

*A clear process turns complex discovery into informed action.*

# FINDINGS NEED CONTEXT

## ***Discovery Is More Valuable When You Understand What the Results Mean***

Finding a potential match is not the same as understanding the risk it represents.

Data discovery can identify a significant number of potential matches. But not every match is a confirmed finding, and not every confirmed finding requires the same response.

## ***S3 Security adds an important layer of human analysis.***

Our engineers review results to eliminate as many false positives as possible before presenting findings to your team. We then work collaboratively with your business and technical stakeholders to evaluate what remains, identify likely confirmed findings, and determine where additional investigation or action may be needed.

This helps your team focus its attention on the findings that matter rather than treating every potential match equally.

## FROM FINDING TO DECISION

Depending on the results, a finding may be:

- ✓ **Ruled out as a false positive**
- ✓ **Confirmed as sensitive information**
- ✓ **Identified for further investigation**
- ✓ **Accepted based on business need**
- ✓ **Selected for remediation**

The result is more than a list of matches. It is a clearer understanding of where sensitive information exists and which findings warrant attention.



***Better analysis leads to better decisions.***

## REMEDiation WITH CONTROL

### *Decide What Should Stay and What Should Change*

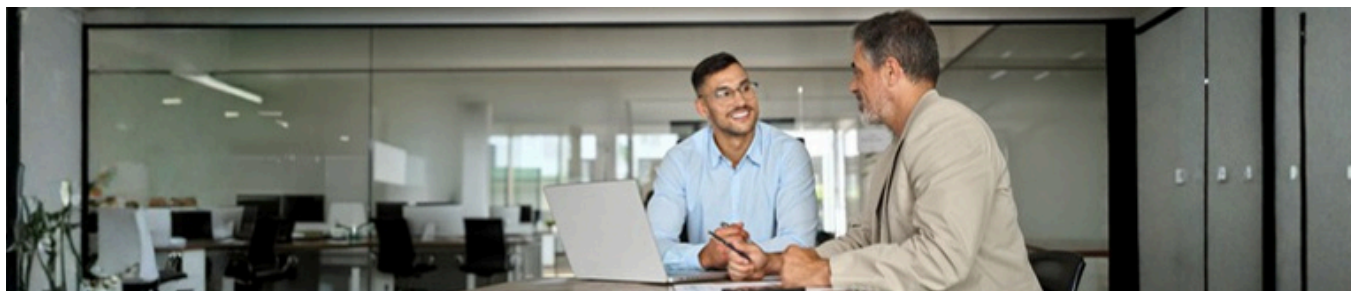
Not every instance of sensitive data represents a problem.

Some information may be located exactly where it belongs and protected appropriately. Other findings may reveal unnecessary copies, data stored in unexpected locations, or information that no longer serves a legitimate business purpose.

S3 Security works with your team to discuss appropriate remediation options for confirmed findings. Depending on the environment, data location, and technical capabilities, supported actions may include deletion or encryption. Where direct remediation is not supported, S3 Security can still review and validate findings to help focus your team's investigation and remediation efforts.

### ***No remediation is performed without client authorization.***

This controlled approach gives your organization the opportunity to investigate findings, consider business requirements, and determine the appropriate action before data is changed or removed.



## FINAL REPORTING

At the conclusion of the engagement, S3 Security provides final reporting that documents:

- **Data identified during the engagement**
- **Findings reviewed and validated**
- **Remediation actions performed, where applicable**
- **Findings that remain outstanding**

This creates a documented view of the environment that can support security, privacy, compliance, and data management initiatives.

***Save time with expert remediation and documentation that supports your compliance and privacy goals.***

## BUILT FOR COMPLEX DATA ENVIRONMENTS

### Visibility Across Dispersed Data

Modern enterprise data rarely exists in one place.

Sensitive information may be distributed across corporate systems, cloud platforms, remote locations, legacy environments, business units, or newly acquired organizations. S3 Security applies a consistent discovery approach across supported targets and locations, helping provide a more complete view of sensitive data across the defined scope.

*Sensitive data remains in its source environment during discovery, helping reduce unnecessary movement of sensitive information.*

### WHEN ENTERPRISE DATA DISCOVERY CAN HELP

#### Compliance & Scope Reduction

Identify sensitive information outside intended environments that may be increasing compliance obligations or risk.

#### Privacy & Data Protection

Gain greater visibility into where personal, health, financial, and other regulated information resides.

#### Data Minimization

Identify unnecessary or obsolete copies of sensitive information that may no longer serve a legitimate business purpose.

#### Mergers & Acquisitions

Gain visibility into sensitive information inherited through an acquisition or distributed across newly integrated entities and environments.

#### Cloud & Technology Transitions

Understand where sensitive information resides as systems and data are migrated or consolidated.

#### Data Governance

Validate where important information is stored and use findings to strengthen governance and protection strategies.

*Greater visibility across complex environments helps reduce risk, support compliance, and guide better business decisions.*

# WHY S3 SECURITY

## Expertise Beyond Discovery

Finding sensitive data is only part of the challenge. Understanding what the findings mean, determining what requires attention, and deciding how to address it takes experience.

S3 Security delivers Enterprise Data Discovery as a managed service, combining powerful discovery capabilities with experienced security professionals who guide the engagement from initial scoping through final reporting.

## WHAT SETS US APART

### A Collaborative Approach

We work alongside your security, compliance, privacy, technical, and business stakeholders to tailor discovery to your environment and priorities.

### Experienced Analysis

Our engineers review findings before they reach your team, helping reduce noise and focus attention on the information most likely to require investigation or action.

### Tailored Scope

Discovery is scoped around your organization, from specific data types and systems to regulatory requirements, business units, or a broader enterprise environment.

### Compliance-Informed Guidance

We help your team evaluate findings and remediation options with business, security, privacy, and compliance requirements in mind.



## GREATER VISIBILITY. MORE INFORMED DECISIONS.

Knowing where sensitive data resides gives your organization a stronger foundation for protecting it, managing risk, and meeting evolving privacy and compliance obligations.

***A managed service reduces the burden on your team while bringing expertise to every stage of discovery.***

# YOUR CYBERSECURITY PARTNER



S|3 SPECIALIZED SECURITY SERVICES

## FLOAT ON

Cybersecurity and compliance to ward off any threat.

### *Across Your Environment, We Help Bring Sensitive Data Into View*

Whether you are reducing compliance scope, supporting privacy initiatives, integrating an acquisition, or simply trying to better understand where sensitive data resides, S3 Security is here to help.

Our Enterprise Data Discovery service combines broad discovery capabilities with experienced analysis and practical guidance. S3 Security manages the process from scoping through review and approved remediation, helping reduce the burden on your internal team while providing clear reporting of the results.

With more than 25 years of experience helping organizations navigate evolving security and regulatory demands, S3 Security brings the expertise and partnership needed to help you better understand, manage, and protect sensitive information.

#### QUICK LINKS TO S3 SECURITY CERTIFICATIONS

[CMMC Authorized C3PAO](#)

[PCI QSA](#)

[CMMC RPO](#)

[PCI ASV](#)

[CREST Pathway+](#)



#### CONTACT US

972-378-5554

[info@s3security.com](mailto:info@s3security.com)  
[www.s3security.com](http://www.s3security.com)

4975 Preston Park Blvd. Ste. 500  
Plano, TX 75093